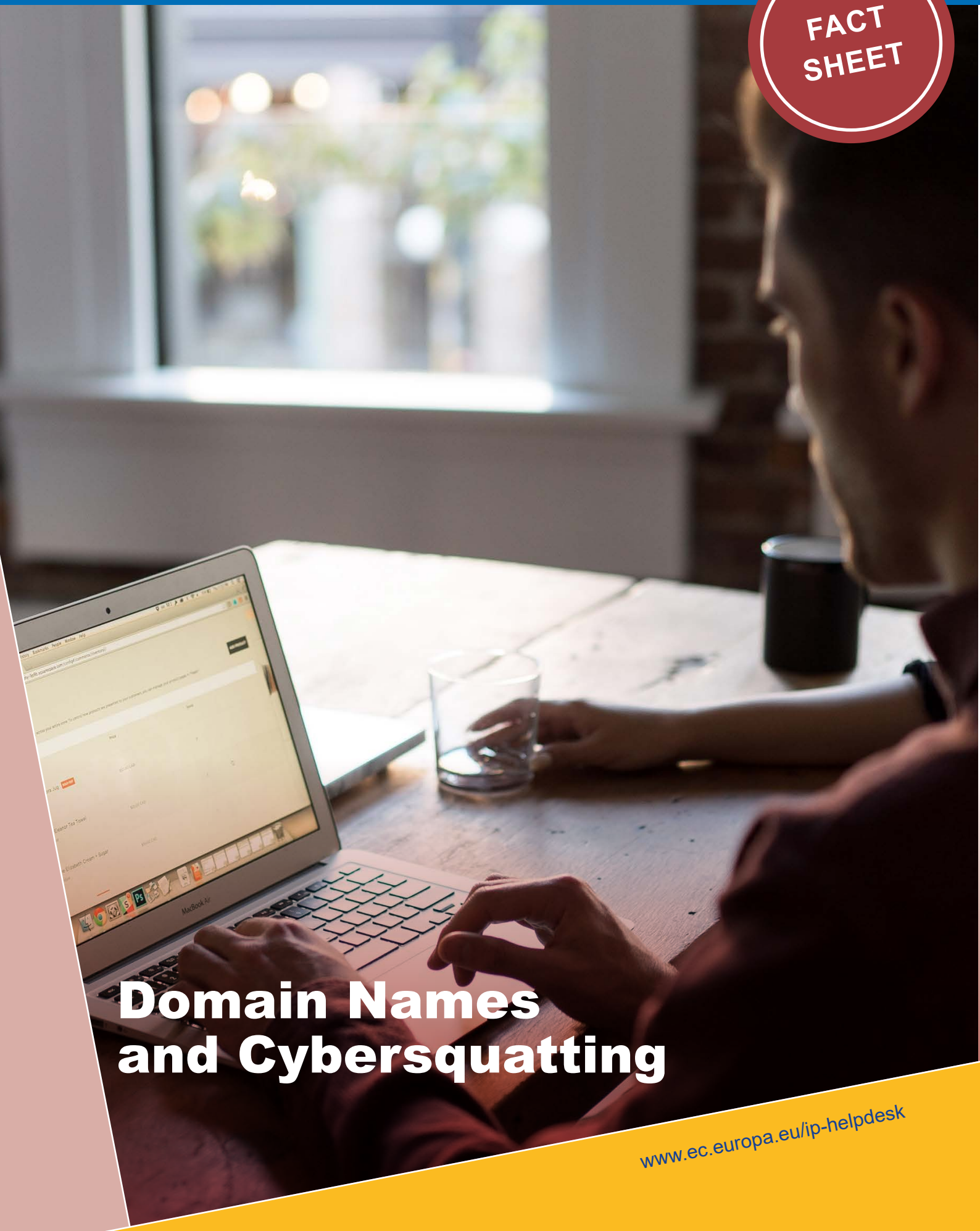
European
IP Helpdesk

FACT SHEET



Domain Names and Cybersquatting

www.ec.europa.eu/ip-helpdesk

Update: September 2022[1]

Summary

1 *This is an updated version of the fact sheet initially developed and first published in November 2017.

Introduction

The Internet has created plenty of opportunities for small and medium-sized enterprises (SMEs), as it has revolutionised the dynamics of international commerce and facilitated internationalisation.

The Internet made it easier for SMEs to gain international market presence comparable to that of large companies, something that previously might not have been affordable due to the amount of resources required. Moreover, the world wide web is an excellent means to boost brand visibility.

Hence, while the Internet is a gateway for SMEs in many ways, it is also an ideal platform for infringers to sell counterfeit products and commit fraud. One of the most significant challenges related to Internet fraud is "cybersquatting" whereby a person or an entity registers, sells, or uses a domain name containing someone else's trademark, product name, or company name without having legal rights to it, often with the ultimate purpose of offering it for sale to its legitimate owner at a much higher price than the domain's registration fees.

This fact sheet aims to introduce the definition of a domain name, how it can be registered, and its relation with trademarks. Moreover, the topic of cybersquatting will be covered. Finally, we will address the available dispute resolution mechanisms that SMEs may use to protect their businesses online.

1. What is a domain name?

According to the World Intellectual Property Organization (WIPO), "domain names are the human-friendly forms of Internet addresses, and are commonly used to find websites"[1]. In other words, they simplify the complicated string of numbers composing the "IP address" (IP stands for Internet Protocol), which is hard to remember by heart.

For example, the domain name "iprhelpdesk.eu" was previously used to locate the European IPR Helpdesk website at www.ec.europa.eu/ip-helpdesk. Apart from this function, domain names also identify a company or a trademark on the Internet.

To translate IP addresses into a more accessible format, they need to be associated with a string of letters (the domain name). This is possible thanks to the Domain Name System (DNS), a global addressing system in charge of translating domain names into IP addresses, and vice versa. It is coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN)[2].

1.1 Domain name levels

Domain names are classified in three hierarchical levels:

- **Top level:** The top level of a domain name is located after the last dot ("."). For example, in "iprhelpdesk.**eu**", the top-level domain is "**eu**".

  There are two types of top-level domains:
  - Generic Top Level Domain (gTLD): indicates the area of activity (e.g., ".com" for any purposes, ".net", ".edu" or ".biz", restricted to businesses).
  - Country Code Top Level Domain (ccTLD): indicates the country or territory in which the domain owner intends to operate (e.g., ".es" for Spain or ".eu"[3] for the European Economic Area).

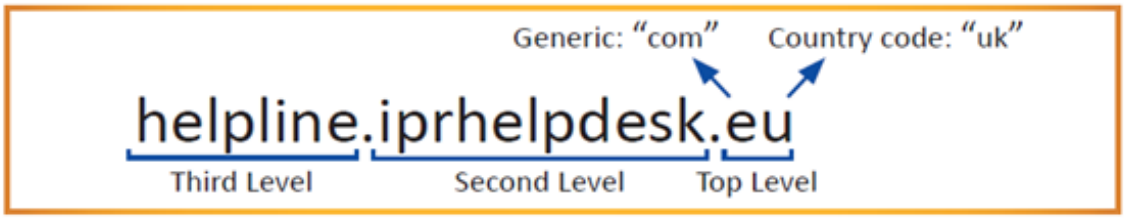
- **Second level:** The second level of a domain name is located directly to the left of the top-level domain. For example, in "**iprhelpdesk**.eu", the second level domain would be "**iprhelpdesk**". Most domain name disputes concern this type of domain.

1 For more information regarding domain names, visit WIPO's FAQs page here.

2 The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit multi-stakeholder association designed to ensure the stable and secure operation of the Internet's unique names systems. It supervises the domain name registration system and provides guidelines and rules to be followed by all accredited registrars. Find out more about ICANN here.

3 For further information regarding ".eu" domain names, check the Commission Regulation (EC) No 874/2004 of 28 April 2004.

- **Third level:** The third level of a domain name, also known as a subdomain, is located directly to the left of the second-level domain. For example, in “helpline.iprhelpdesk.eu”, the third level domain would be “helpline”. Not every address has this level as it is often used to identify the different sections of a website, usually corresponding to different departments in large organisations.



1.2 New gTLDs

In 2011, ICANN launched the so-called **“New gTLD Program”** to expand the domain name system, particularly by making it possible to register new gTLDs – that is, the type of domain located after the last dot and that has no geographical meaning (e.g., .com, .biz, etc.).

Thanks to this initiative, individuals and companies can register their domains under new extensions such as “.guru” or “.book” and trademarks and words in different scripts such as Chinese or Cyrillic.

It must be noted that not everyone can apply for a new gTLD, which is a much more complex process than simply buying a second or third-level domain. **Only established public or private organisations that meet the eligibility requirements can apply to create and operate a new gTLD registry.** Applicants must demonstrate the operational, technical, and financial capability to run a registry and comply with additional specific requirements.

2. How are domain names protected?

2.1 Scope of protection

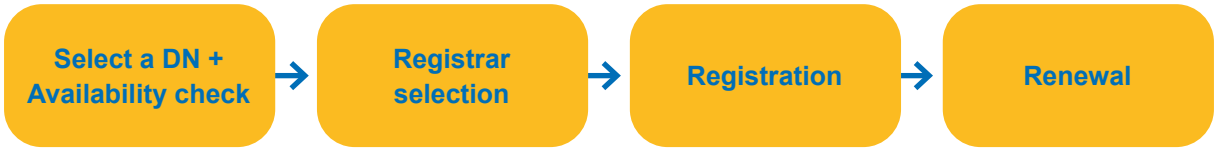
Domain names are usually not considered Intellectual Property Rights (IPRs) – the right acquired by the owner of a domain name is the exclusive right to use it for the duration of a contract with the registrar. Nevertheless, domain names can still be considered intangible assets, just like IPRs (i.e., a non-physical asset with a value, which can give rise to financial rights and interests and thus have an economic value).

The registration of domain names is governed by the first-come, first-served rule. This means that, in principle, anyone can obtain a domain name as long as it is available, meaning that it has not been registered first by someone else. The consequences of this rule are explained in section 3 below.

Unlike other IPRs like trademarks, domain names are not territorial, as they have a worldwide geographical scope. This means that individuals and companies can register their domain names with any accredited registrar in the world, and once the domain name is registered, it has a worldwide effect.

2.2 Registration process

The registration process is straightforward and can be summarised in the following steps:



1) Select a domain name and perform an availability check

Performing a prior search to ascertain whether a domain name is available is a time saver and a highly recommended step. There are several databases, such as WHOIS or EURid, where one can easily determine whether a domain name is available or, on the contrary, whether it has already been registered in advance. In the latter case, the details of the domain name owner are usually public, which increases transparency and, at the same time, facilitates transactions of domain names. Furthermore, it is worth mentioning that domain names are usually used as trademarks, therefore conflicts may arise between trademarks and domain names. Hence, if a domain name is intended to be used also as a trademark, it is advisable to perform a prior trademark search in the appropriate database such as e-Search plus or TMview to verify its availability[4].

4 For further information on trademark application and searches, see the European IPR Helpdesk factsheet "Trademarks: The Face of Your Business", available here.

2) Registrar selection

Any individual or company that wishes to register a domain name under a gTLD may do so through an ICANN-accredited registrar. There are hundreds of accredited registrars located throughout the world, a list of which can be accessed here.

3) Registration

Registrants have the choice to determine the duration of their domain name registration. Usually, registrars offer the possibility to register domain names for one year or for multi-year periods, up to 10 years.

4) Renewal

Usually, registrars offer the possibility to renew domain names indefinitely. It is important to check the rules of each individual registrar as regards renewals.

If the registrant does not renew its domain name, it will expire[5]. It is important to check the deadlines with your registrar, although they must send you two renewal reminders. If the domain name renewal request is not filed in due time, there are three possible consequences:

- **Loss of the domain name.** This means that it will not be possible to have the domain name back and, therefore, it will be available for everyone.

- **Option to renew.** Within 45 days after expiration, it might be possible to renew the expired domain name, as far as it is foreseen in the contract with the registrar.

- **Option to restore.** If the registrar deletes the expired domain name, it is still possible to restore it in a 30-day period, following the deletion.

5 For additional information, check FAQs for Registrants: Domain Name Renewals and Expiration.

3. Cybersquatting: The conflict between domain names and trademarks

While the Internet has become an essential tool for business development, it has at the same time created a growing number of potential threats for trademark owners.

The Internet provides a scenario in which creating and disseminating content has become easier than ever. Furthermore, as explained above, registering domain names is simple, affordable and fast. Lastly, the proliferation of the new gTLDs has substantially increased the possibilities for new domain name variations.

While this can boost business dynamics and is appreciated by companies, it can also be a potentially harmful threat. There are two main different ways in which trademark owners can see their rights infringed on the Internet:

- by having their **trademarks replicated on third party websites**, creating confusion among consumers regarding the origin of the goods or services advertised on those websites (e.g., a trader sells counterfeited products online)[6], or
- by having **their trademarks registered as domain names by unauthorised third parties**, a practice known as cybersquatting (e.g., an individual registers a third-party trademark as a domain name in the ".com" extension, for example, without any right to do so).

Cybersquatting is a practice through which abusive registrations of domain names that are already registered, either as domain names in one or more top-level extensions, or as trademarks or trade names. Cybersquatters register such domain names and offer them for sale later – often to the owner of the earlier domain name or trademark – at a higher price than the original registration fee.

While the first-come, first-served rule applies in domain name registration, the actions of cybersquatters do not remain unpunished. There are different means to solve the disputes that can arise in this area, as well as a preventive system for avoiding trademark infringement by domain name registrants, which is also a first step before resorting to dispute resolution procedures: the Trademark Clearinghouse (TMCH)[7].

The TM Clearinghouse is a right protection mechanism that allows trademark owners to record their trademark information into a database. In this way, it grants priority access to trademark owners for registering new gTLDs. Moreover, it warns third parties seeking to register a domain name of the existence of an identical trademark and notifies the trademark owner in case of such a registration.

6 Consult the European Commission's "Communication on Tackling Illegal Content Online – Towards an enhanced responsibility of online platforms".

7 For further information about the Trademark Clearinghouse, click here.

4. Domain name dispute resolution procedures

As explained above, domain name disputes usually arise between a trademark owner and a domain name registrant who has registered a domain name that might be infringing the rights of a trademark owner.

In this scenario, a trademark owner, known as the complainant in this type of disputes, will try to either gain control over the infringing domain or seek for its suspension, thus preventing the other party from using it. These disputes can be solved by a court. However, in order to avoid the costs[8] and delays usually associated with court proceedings, it is advisable to resort to the domain name dispute resolution proceedings available, managed by ICANN.

4.1 Uniform Domain Name Dispute Resolution Policy[9]

The Uniform Domain Name Dispute Resolution Policy (UDRP) is a system established by ICANN for the resolution of disputes regarding the abusive registration and use of domain names.

It is applied by all accredited registrars in their agreements with customers (domain name holders or registrants). During the domain name registration procedure, registrants declare not to infringe the rights of third parties and accept to submit themselves to the UDRP. This means that, in the case where a domain name registration is considered to be abusive, the third-party trademark owner could decide to bring an UDPR proceeding against the alleged infringer. The latter shall be bound to be subject to the above-mentioned proceeding, as it agreed to undergo it at the time it registered the domain name.

This does not mean that the complainant does not have other options, such as court proceedings, to solve the dispute. The choice of the relevant forum remains the complainant's decision, and the registrant, as a defendant in this scenario, has no say in it.

The complainant in a UDRP case must prove that:

1. the domain name is identical or confusingly similar to a trademark or a service mark in which the complainant has rights;
2. the registrant has no rights or legitimate interests in respect of the domain name; and
3. the domain name has been registered and is being used in bad faith.

8 While domain name dispute resolution proceedings are not free of charge, they are usually less costly than court proceedings.
9 To find out more about the rules governing UDRP proceedings, click here.

How can bad faith be proved?

The complainant should submit evidence to prove any circumstances showing bad faith on the registrant's side. Below, you will find a non-exhaustive list of examples of circumstances that would be considered as bad faith in a UDRP case:

- the domain name was registered mainly in order to be sold to the complainant, who is the owner of the trademark, or to a competitor of that complainant for a higher price than the registration costs paid;
- the domain name was primarily registered for the purpose of disrupting the business of a competitor;
- by using the domain name, the registrant intentionally attempted to attract Internet users to their website or other online location for financial gain, by creating a likelihood of confusion with the complainant's trademark as to the source, sponsorship, affiliation, or endorsement of the registrant's website or location or a product or service on the registrant's website or location.

As mentioned above, **the UDRP procedure is much shorter than court proceedings**. It usually takes 60 days from the date the complaint is received by the dispute resolution service provider[10] for a case to be concluded.

The application process is relatively simple. The complainant must address the complaint to a dispute resolution service provider following the UDRP Rules, which, among other things, require the complaint to contain:

- the complainant's choice of panel – single member or three member panel[11];
- the domain name subject of the complaint;
- the registrar with whom the domain name is registered;
- the trademark(s) or service mark(s) on which the complaint is based and the goods and services with which the trademark is used;
- the grounds on which the complaint is made;
- the remedies sought.

Under UDRP, there are two available remedies for complainants: cancellation of the domain name or transfer of the domain name to the complainant. The parties to UDRP proceedings are not prevented from submitting the dispute to a court for independent resolution during or after the UDRP proceedings. In such cases, the decision made under the UDRP will not be implemented by the registrar and, subject to compliance with the applicable formalities under UDRP, the decision of the court will prevail.

10 UDRP cases are handled by administrative-dispute-resolution service providers, listed here.

11 The panel is the individual or group of individuals, known as "panelists", appointed to decide on a UDRP case.

4.2 Uniform Rapid Suspension System[12]

The Uniform Rapid Suspension System ("URS") is a system established by ICANN, **only applicable to new gTLDs** (such as .companyX or .city) to protect the rights of trademark owners in a **low-cost and fast way**. This system complements the UDRP system and it is used in the most blatant cases of trademark infringement, perpetrated by domain name registrants. These cases have no questions of fact left open, but they are clear cases of trademark abuse (such as counterfeiting, massive fraud or the spread of virus/malicious software).

Similar to the UDRP system, the complainant in a URS case must prove that:

1. the registered domain name is identical or confusingly similar to the complainant's trademark;
2. the domain name registrant has no legitimate right or interest in the domain name; and
3. the domain name was registered and is being used in bad faith.

The URS is an expedited system. The deadlines are much shorter than those in the UDRP. Usually, the whole procedure can be solved with a final decision within a month. It is worth mentioning that, throughout the procedure, the infringing domain is locked until a final decision has been issued[13].

As in UDRP, the application process is quite simple and the complaint is required to contain essentially the same elements, following the URS Rules.

Furthermore, the examiner makes a decision simply by analysing the documents submitted by the parties with the complaint and the response, without any additional gathering of evidence or a hearing. This certainly facilitates the expedited resolution of the conflict.

It must be noted that the domain name is not transferred under the URS to the complainant in those cases in which the latter is successful, as it is under the UDRP. Only two solutions are possible under the URS: if the complainant is successful, the suspension of the domain[14] or the return of the domain to the registrant if the latter is the one being successful. **Consequently, this procedure should only be used by those trademark owners who are not interested in gaining ownership of the infringing domain name, but rather wish to stop said infringement as soon as possible.**

As under the UDRP, the conclusion of the URS procedure allows the parties to also submit the dispute to the UDRP or to a competent court in certain instances.

12 To find out more about the rules governing the URS procedure, click here.

13 URS cases are handled by URS providers, which are organisations approved by ICANN for these purposes. A list of providers can be found here.

14 The domain name is suspended for the remainder of the registration period, during which the domain name will become available again for registration on a first-come, first-served basis.

4.3 Trademark Post-Delegation Dispute Resolution Procedure[15]

The Trademark Post-Delegation Dispute Resolution Procedure ("PDDRP") is a domain name dispute resolution procedure established by ICANN, **only applicable to new gTLDs**, for cases in which **a domain name owner believes that a registry operator, such as an organisation that manages the registration and operation of domain names, is intentionally and systematically infringing trademarks in its top-level domain**, either by itself or by assisting third parties in doing so[16].

Similar to other dispute resolution procedures, the complainant must prove the registrant's bad faith and obtain unfair advantage from the reputation of the complainant's trademark. Moreover, evidence must show that the registration can be harmful for the trademark's reputation or it can create a risk of confusion with the complainant's mark. This means it is not enough to show that the registry operator is aware of possible trademark infringement through registration in the gTLD.

The application process is similar to the UDRP and URS but it has some specificities related to the nature of the disputes under these proceedings, which are detailed in the Trademark Post-Delegation Dispute Resolution Procedure Rules. Considering that the defendant is a registry operator, the complainant is required to provide a statement in which a relation between the harm suffered and the resulting actions must be shown.

Different enforcement measures can result from the procedure if the registry operator is found liable under the PDDRP, from an obligation for the registry to implement remedies in order to prevent future infringing registrations to the total termination of the registry agreement with ICANN.

4.4 Legal Rights Objection[17]

The Legal Rights Objection (LRO) is a dispute resolution procedure under which trademark owners and intergovernmental organisations (i.e. those that meet the criteria for registration of a .int domain name) can formally object to a new gTLD application on the basis of a "Legal Rights Objection". In other words, before ICANN approves a new gTLD, trademark owners or the intergovernmental organisations involved, the trademarks or names or acronyms of which may be infringed by the new gTLD, can stop the approval of the new gTLD[18].

Similar to other dispute resolution procedures under this section, the objector (i.e. the party that objects to the new gTLD application) will have to prove that the potential use of the gTLD sought takes unfair advantage of the distinctive character or the reputation of the objector's trademark, name or acronym, unjustifiably impairs the distinctive character or the reputation of the objector's mark or name or acronym, or creates a likelihood of confusion between the gTLD applied for and the trademark, name or acronym.

15 To find out more about the PDDRP, consult the applicable rules here.
16 PDDRP cases are handled by external providers, other than ICANN. A list of providers can be found here.
17 For more information on LRO, visit WIPO's website and Module 3 of the new gTLD Applicant Guidebook.
18 LRO cases are handled by external providers, other than ICANN. A list of providers can be found here.

The application process to have a dispute solved under LRO is similar to the application for the above-mentioned proceedings, but it has some particulars related to the nature of the disputes under these proceedings, which are detailed in ICANN's new gTLD Dispute Resolution Procedure, including a statement on the grounds upon which the objection is being filed and an explanation of the validity of the objection and why it should be upheld. The remedies are limited to the success or dismissal of the objection, with no monetary damages other than the possibility for the prevailing party to obtain a partial refund of the panel fee.

The above-mentioned procedures are summarised below:

	Type of dispute	Duration	Possible outcomes
UDRP	- Trademark owner v. - Domain name registrant	2 months	- Domain returned to registrant - Domain transferred to complainant - Domain cancelled
URS	- More expedited version of UDRP - Only for new gTLDs	1 month	- Domain suspended - Domain returned to registrant
PDDRP	- Trademark owner v. - Registry operator - Only for new gTLDs	8 months	Different measures against the registry operator
LRO	Objection of trademark owners and intergovernmental organisations to new gTLD applications	2 months	- Success of the objection - Dismissal of the objection

Advantages of domain name dispute resolution procedures

- Expedited
- Impartial
- Affordable (low fees, no attorney required)
- Limited results (transfer/cancellation)
- Direct enforcement by the accredited registrars
- Transparent: the proceedings and decisions are published on the Internet
- Possibility to bring the case to court after the proceedings.

Conclusion

Generally speaking, choosing a domain name is simple. If it is easy to remember, short, and catchy, it may be a recipe for success. But even if the choice is brilliant from a marketing standpoint, it may not be so from a legal perspective. Registering a domain name that is in conflict with a trademark or commercial name puts the registrant at risk of legal proceedings and, sometimes, the loss of the domain name. That, together with an often significant investment in developing a website, can constitute a blow for a company.

However, a legitimate owner of a domain name has to be aware of the risks of the practice of cybersquatting and of any available defences against it.

In order to be on the safe side when choosing a domain name, one has to remember, among other aspects, to perform a prior search in order to ascertain whether the domain name intended to be registered is available. At the same time, trademark holders should be aware of the dispute resolution procedures that can assist them in case of cybersquatting.

Useful Resources

For further information, see also:
- IP Special "IP in Websites"
- Fact sheet "Trademarks: The Face of Your Business"
- Beginner's Guide to Domain Names
- .eu domain names
- Domain Name Dispute Resolution Service
- Uniform Rapid Suspension System
- Trademark Post-Delegation Dispute Resolution Procedure
- Legal Rights Objection
- New Generic Top-level Domains
- Trademark Clearinghouse

Our main goal is to support cross-border SME and research activities to manage, disseminate and valorise technologies and other IP rights and assets at an EU level. The European IP Helpdesk enables IP capacity building along the full scale of IP practices: from awareness to strategic use and successful exploitation.

WEBSITE

The heart of our service portfolio to keep you updated

HELPLINE

Our Helpline team answers your individual IP questions

TRAINING

Gain IP knowledge in our free online and on-site training sessions

PUBLICATIONS

Detailed IP knowledge provided through our high level publications

AMBASSADORS

Our regional ambassadors provide IP support throughout Europe

EVENTS

Meet us at key networking and brokerage events and conferences

Disclaimer

The European IP Helpdesk is managed by the European Commission's Executive Agency for Small and Medium-sized Enterprises (EASME), with policy guidance provided by the European Commission's Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG Grow).

The information provided by the European IP Helpdesk is not of a legal or advisory nature and no responsibility is accepted for the results of any actions made on its basis. Moreover, it cannot be considered as the official position of EASME or the European Commission. Neither EASME nor the European Commission nor any person acting on behalf of EASME or of the European Commission is responsible for the use which might be made of this information.

© European Union, 2022

Luxembourg: Publications Office of the European Union, 2022
Print: ISBN 978-92-9469-355-6 DOI 10.2826/41052 EA-08-22-176-EN-C
PDF: ISBN 978-92-9469-356-3 DOI 10.2826/715417 EA-08-22-176-EN-N

Get in touch with us.

European IP Helpdesk
c/o Eurice GmbH
Heinrich-Hertz-Allee 1
66368 St. Ingbert, Germany

Web www.ec.europa.eu/ip-helpdesk
Email service@iprhelpdesk.eu

Phone +34 965 90 9692 (Helpline)

Fact Sheet

Publications Office of the European Union